IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method for protecting against manipulation of a motor vehicle controller, the motor vehicle controller comprising at least one microcomputer and at least one memory module, at least one of the at least one memory module constituting a reversible read-only memory said method comprising:

encrypting data by an encryption process;

storing said encrypted data in the reversible read-only memory;

wherein said encrypting step comprises using a key in the encryption process, and said key comprises at least one part of at least one original identifier of at least one module, said module selected from the group consisting of the at least one memory module and the at least one microcomputer of the control device, which identifier is specific to said at least one [[the]] module.

2. (Currently Amended) The [[process]] method as claimed in claim 1, wherein the identifier constitutes the identifier of the microcomputer.

3. (Currently Amended) The [[process]] method as claimed in claim 1, wherein the identifier constitutes the identifier of the at least one memory module.

4. (Currently Amended) The [[process]] method as claimed in claim 1, wherein the key is stored in RAM of the microcomputer.

5. (Currently Amended) The [[process]] method as claimed in claim 1, further comprising reading out at least part of the at least one memory module of the control device to generate a key for encryption of data on a reversible read-only memory from a read-protected OTP area of the microcomputer.

6. (Currently Amended) The [[process]] method as claimed in claim 1 further comprising re-generating a key for decryption of the data which have been stored encrypted in the reversible read-only memory, each time the control device is started up.

7. (Cancelled)

8. (Previously Presented) A method for protecting against tampering with a device, said device comprising plurality of components, each component associated with an identifier, said method comprising:

reading an identifier associated with one of said plurality of components;

generating a decryption key from said at least one identifier;

decrypting data stored in a memory unit with said key; and

comparing said decrypted data with stored data.

9. (Previously Presented) The method of claim 8, further comprising:

generating a reference key from a reference identifier associated with a component;

encrypting said reference identifier with said reference key, and

storing said encrypted reference identifier as said stored data.

10. (Previously Presented) The method of claim 9, wherein said storing step comprises inputting said stored data into an EEPROM.

11. (Previously Presented) The method of claim 9, further comprising permitting access or activation of said component if said decrypted data is identical to said encrypted reference identifier.